## REMARKS

Claims 1, 5, 7, 10, 16, 18, 23, 25, 27, 34-35, 38, 43-45, 50-51, and 57-65 have been amended. Claims 1-65 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

### Section 103(a) Rejections:

The Examiner rejected claims 1, 2, 4, 5, 13-16, 18, 19, 21-23, 30, 33-44, 49-51 and 56-65 under 35 U.S.C. § 103(a) as being unpatentable over Chen et al. (U.S. Patent 6,763,365) (hereinafter "Chen") in view of Bhushan et al. (U.S. Publication 2002/0174157) (hereinafter "Bhushan"), claims 3, 20, 45 and 52 as being unpatentable over Chen and Bhushan and further in view of Lasher et al. (U.S. Patent 4,863,247) (hereinafter "Lasher"), claims 6-12, 24-29, 31, 32, 47, 48, 53, 54 and 55 as being unpatentable over Chen and Bhushan and further in view of Stribaek et al. (U.S. Patent 7,181,484) (hereinafter "Stribaek"), claim 17 as being unpatentable over Chen and Bhushan and further in view of Chen et al. (U.S. Patent 6,687,725) (hereinafter "Chen2"), and claims 46 and 47 as being unpatentable over Chen, Bhushan and Lasher and further in view of Stribaek. Applicants respectfully traverse these rejections for at least the following reasons.

Regarding claim 1, contrary to the Examiner's assertion, the cited art fails to teach or suggest *in response to executing a single arithmetic instruction of a processor instruction set, multiplying a first number by a second number; and adding implicitly a partial result from a previously executed single arithmetic instruction of the processor instruction set to generate a result that represents the first number multiplied by the second number summed with the partial result, wherein the partial result comprises a high order portion of a result of the previously executed single arithmetic instruction.* The Examiner submits that this entire collection of limitations is taught in Chen, col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage"), and col. 10, lines 13-26 (noting only, "multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A, B"). These scant teachings can hardly be said to disclose the above-noted specific aspects of Applicants' claimed invention. Given that above cited portions of Chen clearly do not describe the claimed features, the Examiner has failed to fully and clearly state his ground of rejection of claim 1 and has therefore failed to establish a *prima facie* case of obviousness. The Examiner's remarks (quoted above) refer only generally to features that he believes are taught by the cited passages of Chen without describing how he believes these passages (or elements described therein) teach each of the above-referenced limitations of claim 1. Since the features noted by the Examiner do not correspond to the language and meaning recited in the above-referenced claim limitations, it is not clear or how the Examiner interprets the cited passages to teach the specific limitations of claim 1 as arranged in the claim. The statute clearly places the burden of proof on the Patent Office to prove a *prima facie* rejection. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S. 1057 (1968). The Examiner's vague assertions, which lack a clear mapping between the teachings of Chen and Applicants' claim, cannot be said to establish a *prima facie* case of obviousness.

In addition, Applicants assert that the cited passages clearly do not teach or suggest the above-referenced limitations of Applicants' claim. For example, nothing in the cited passages describes *in response to executing a single arithmetic instruction of a processor instruction set, multiplying a first number by a second number; and adding implicitly a partial result from a previously executed single arithmetic instruction of the processor instruction set*, as recited in claim 1. The "multiplication with feedback" described in the cited passages of Chen appears to refer to feedback within a circuit while executing a single multiplication instruction. For example, the cited passage in col. 11 describes the multiplication operation "AB mod N." In Chen, a hardware circuit may execute this single multiplication operation in two phases. **However, there is no feedback of a partial result from a previously executed single arithmetic instruction of the processor instruction set (i.e. a different instruction) described.** The Examiner's citation in col. 10 describes the operation of Chen's hardware circuit in more detail, but also does not teach or suggest feedback of a partial result from a previously executed single arithmetic instruction, as required by Applicants' claim.

In the Office Action mailed December 10, 2008, the Examiner submits, "Bhushan discloses wherein a previously executed single arithmetic instruction to generate a result. (see Bhushan paragraph [0116], lines 14-20; instruction requires an operand, a result from a previous instructions, the result may be bypassed under the direction of bypass routing control)". **However, Bhushan is directed to a method and apparatus for performing equality comparisons in redundant form arithmetic, and has absolutely nothing to do with the limitations recited in Applicants' claim.** More specifically, Bhushan is directed to a method for bypassing standard output routing from a functional unit. This bypass mechanism allows the result of an addition or subtraction instruction performed while in redundant form to be made available to a comparison instruction (comparing the result with 0 or another value) without converting the result of the addition or subtraction out of redundant form and then back into redundant form for use as an operand of the comparison instruction. The cited passage in Bhushan describes this bypass mechanism.

**Applicants assert that the bypass mechanism of Bhushan, even if combined with Chen, teaches nothing about the above-referenced limitations of Applicants' claim.** For example, Bhushan describes nothing about implicitly adding a partial result of a previous instruction as part of performing a single arithmetic instruction (i.e., as an implicit operand). Instead, Bhushan describes that if the result of a single arithmetic instruction happens to be explicitly specified as an operand of a subsequent comparison operation, the entire result of the single arithmetic instruction may be passed to a functional unit that is to perform the subsequent comparison instruction without passing it through a redundant conversion unit and/or register file. Therefore, at most, Bhushan teaches a method for more efficiently passing the entire result of an arithmetic instruction to the input of a subsequent non-arithmetic (comparison) instruction, in response to the result being explicitly coded as an operand for the comparison operation. This clearly does not teach or suggest implicitly adding a partial result of a previously executed single instruction of a processor instruction set in response to executing a (different) single arithmetic instruction of the processor instruction set, as in Applicants' claim. In addition, Bhushan does not teach or suggest that this bypass mechanism can be used in any situation other than when an arithmetic instruction is followed by a comparison instruction in which the result of the arithmetic instruction is to be compared to zero or another value. Such a situation is clearly not analogous to the limitations recited in Applicants' claim regarding execution of a single arithmetic instruction that results in a partial result of a previous arithmetic instruction being implicitly added to the product of two other numbers.

Further regarding claim 1, the cited art fails to teach or suggest *storing at least a portion of the generated result; and using the stored at least a portion of the generated result in a subsequent computation in the cryptography application*. As in the previous Actions, the Examiner submits that these limitations are taught by Chen in col. 4, lines 8-11 (noting only, "multiplication and addition are performed by large circuits"); in col. 10, lines 13-36 (without including any remarks regarding this passage); and in col. 11, lines 34-40 (noting only, "feedback; first using circuit; then using circuit again with register provided with output from first operational stage (multiplication with feedback)"). The Examiner has again failed to explain how he believes the cited passages teach the above-referenced limitations. Applicants again assert that since they have nothing to do with storing a portion of the generated result (i.e., the result of the multiplying and adding recited in claim 1), nor with using the stored portion in a subsequent computation in a cryptography application, they clearly do not teach the above-referenced limitations of claim 1. Instead, this passage again appears to describe the execution of a single multiplication instruction. In addition, in the passages cited by the Examiner in Bhushan, the result of an addition or subtraction instruction that is to be used in a subsequent comparison instruction is explicitly not stored, due to the bypass mechanism described above. **Therefore, Bhushan actually teaches the opposite storing a result of one instruction for use in a subsequent computation.**

On pages 3-4 of the Response to Arguments section of the Final Action mailed June 26, 2009, the Examiner submits, "Bhushan prior art discloses that if a current instruction requires the result from a previous instruction. The result can be supplied. This disclosure indicates that the results of one instruction are saved and used as input or as an operand for a next instruction. There is an additional option where the result may be bypassed. But, the result may also be used." **Applicants note that the Examiner has not cited any portion of Bhushan to support his remarks regarding the saving of a result (or a partial result) for use in a subsequent instruction.** Various passages of Bhushan describe that control logic can be used to select for input to a compare circuit either an operand of a compare instruction (i.e. an operand explicitly encoded in the compare instruction) or a bypassed result of an addition or subtraction operation. Nothing in Bhushan describes storing at least a portion of a generated result and using the stored portion of the generated result in a subsequent computation, as required by Applicants' claim. Instead, in the case that an operand is selected as the input to the compare instruction, this operand is clearly not the result of a previous instruction, as suggested by the Examiner, but is an operand explicitly specified in the compare instruction itself. And in the case that a result of an addition or subtraction instruction is selected as the input to the compare instruction, the result is fed to the compare circuit using a bypass mechanism, as discussed above. Furthermore, in neither of these cases is at least a portion of a result generated by a single arithmetic instruction stored and used in a subsequent computation in a cryptography application, much less a portion of a result generated using the operations recited in Applicants' claim. Applicants again assert that Bhushan, whether considered alone or in combination with Chen, clearly fails to disclose these limitations of Applicants' claim.

On page 2 of the Response to Arguments section of the Final Action mailed June 26, 2009 (in remarks directed to claim 18), the Examiner submits, "Applicant's claimed invention is a sequence of arithmetic process steps (multiplication, addition, subtraction) performed and designated at completion as a single arithmetic instruction" (emphasis added). **The Examiner is clearly mischaracterizing Applicants' claimed invention.** Applicants' independent claims explicitly recite executing a single arithmetic instruction, and have been further amended to clarify that this single arithmetic instruction is an instruction of the processor's instruction set. It is clear from the plain language of these claims, as well as the title, abstract, and description in Applicants' disclosure, that these claims are directed to a specific, individual instruction of a processor's instruction set that supports public-key cryptography by causing the processor to perform the recited arithmetic operations. Applicants remind the Examiner that, "All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP 2143.03; *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). The Examiner cannot simply ignore the wording of a claim in order to support his interpretation. The plain language of the claims requires that the operations recited in these claims be performed by the processor in response to execution of a single arithmetic instruction of the processor's instruction set. **This is clearly not taught by the cited references, whether they are considered alone or in combination.** Various ones of the dependent claims recite limitations of other single arithmetic instructions of the processor's instruction set, which are also not taught by the cited references, whether they are considered alone or in combination.

**As discussed above, the descriptions of individual features listed by the Examiner do not teach the specific combination of limitations recited in claim 1, as arranged in the claim.** The Examiner is clearly attempting a piecemeal reconstruction of Applicants' invention in hindsight without consider the claimed invention as a whole. Such reconstruction is improper. *See, e.g., Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985). For example, a general reference to "multiplication with feedback" and a description of a hardware circuit usable to execute a single multiplication instruction clearly do not teach the specific limitations recited in claim 1 regarding a single arithmetic instruction of a processor instruction set that, when executed, results in *multiplying a first number by a second number; and adding implicitly a partial result from a previously executed single arithmetic instruction of the processor instruction set*. In another example, the Examiner's statement that "multiplication and addition are performed by large circuits" teaches nothing about the limitations recited in claim 1. Furthermore, the addition of the Bhushan reference, which describes a mechanism to bypass a conversion operation used in completely non-analogous situations, teaches nothing about Applicants' claimed invention.

Finally, the Examiner has not stated a proper reason to combine the teachings of the cited art. The Examiner submits that it would have been obvious to one of ordinary skill in the art "to modify Chen for a previously executed single instruction to generate a result as taught by Bhushan... in order to provide an efficient method for an uncomplicated arithmetic circuit that is capable of adding or subtracting numbers in redundant from and comparing a result without requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5." **Applicants assert that this passage merely describes a benefit of using Bhushan's own methods for performing <u>equality comparisons in redundant number form</u>. It has absolutely nothing to do with a benefit that may be applicable in the system of Chen or with the above-referenced limitations of Applicants' claim, both of which are directed to instructions involving <u>multiplication operations</u>.** Therefore the rejection is improper. In addition, there is nothing in Bhushan or Chen that teaches or suggests that Bhushan's method could be combined with the system of Chen in a way that would result in Applicants' claimed invention, since neither reference teaches the above-referenced limitations of Applicants' claim. In fact, it is not clear that it is even possible to combine the teachings of Chen and Bhushan, as suggested by the Examiner, since they are directed to completely different problem spaces and corresponding solutions. Thus, one of ordinary skill would not have combined the teachings of Bhushan with the teachings of Chen in the manner proposed by the Examiner.

To establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. As discussed in detail above, neither of the cited references teaches or suggests the above-referenced limitations of Applicants' claim, whether taken alone or in combination, and the Examiner has failed to state a proper reason to combine the references in teaching Applicants' claimed invention. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

For at least the reasons above, the rejection of claim 1 is unsupported by the cited art and removal of the rejection thereof is respectfully requested.

Independent claims 43, 57, and 64 include limitations similar to those recited in claim 1 and discussed above, and were rejected for similar reasons. Therefore, the arguments presented above apply with equal force to these claims, as well.

Independent claim 18 includes limitations similar to those recited in claim 1 and discussed above, and was rejected for reasons similar to those discussed above regarding claim 1. In fact, the Examiner includes several of the same citations and notes several of the same features of Chen and Bhushan in rejecting claim 18. Therefore, Applicants traverse this rejection for at least the reasons presented above regarding limitations in this claim that are similar to those in claim 1.

**In addition**, claim 18 recites *adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number*. On page 2 of the Response to Arguments section of the Final Action mailed June 26, 2009, the Examiner submits, "Applicant's claimed invention is a sequence of arithmetic process steps (multiplication, addition, subtraction) performed and designated at completion as a single arithmetic instruction" (emphasis added). **As discussed above, the Examiner is clearly mischaracterizing Applicants' claimed invention.** The plain language of the claim requires that the operations recited in this claim (including that recited in the above-referenced limitation) be performed by the processor in response to execution of a single arithmetic instruction of the processor's instruction set. **This is clearly not taught by the cited references, whether they are considered alone or in combination.**

The Examiner goes on to repeat his assertion that Chen discloses the same arithmetic process steps (multiplication, addition, subtraction) and the concept of feedback by whereby a circuit using feedback is defined as, "the transfer part of the output of an active circuit or device back to the input." **Applicants assert that this definition of "a circuit using feedback" is not disclosed in either reference, nor is it relevant to the patentability of Applicants' claims.** Applicants' claims are not directed to "a circuit using feedback" in general, but to specific limitations regarding the implicit addition of a partial result of one single arithmetic instruction of a processor's instruction set when executing a different single arithmetic instruction of the processor's instruction set. The Examiner further submits, "The concept and usage of feedback enables the processing of a sequence of arithmetic process steps as a single arithmetic operation or instruction. In feedback, the output of one arithmetic process step is input to a next arithmetic process step in a sequence of arithmetic processing steps. The completion of the set of multiple processing steps results in the completion of a single arithmetic complex operation or instruction. This claim limitation indicates a sequence of arithmetic process steps resulting in completed arithmetic operation. The concept of feedback enables a sequence of arithmetic process steps such as multiplication and addition operations to be performed. The concept of feedback allows the output of a process steps to be used as input for a next process step. The single arithmetic operation or instruction would be the completion of the set of arithmetic processing steps."

Applicants assert that the Examiner's references to the "concept of feedback" can hardly be said to disclose the above-noted specific limitations of Applicants' claimed invention. For example, the Examiner has not explained how the cited art can be said to teach the specific limitations regarding a single arithmetic instruction of a processor's instruction set that, when executed, causes a device to use a stored result (or portion thereof) in a subsequent computation, where the stored result is generated by the device multiplying a first number by a second number, and adding implicitly a partial result from a previously executed single arithmetic instruction of the processor instruction set, wherein the partial result comprises a high order portion of a result of the previously executed single arithmetic instruction, and adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number, and storing at least a portion of the generated result **in response to execution of a single arithmetic instruction of a processor's instruction** set, as claimed. **No such single arithmetic instruction is taught or suggested by either reference, and nothing about the bypass mechanism of Bhushan teaches anything about a single arithmetic instruction that, when executed, results in performance of the operations recited in claim 18**. Since the features noted by the Examiner do not correspond to the language and meaning recited in the above-referenced claim limitations, it is not clear how the Examiner can interpret the cited passages to teach the specific limitations of claim 18 as arranged in the claim.

For at least the reasons above, the rejection of claim 18 is unsupported by the cited art and removal of the rejection thereof is respectfully requested.

Claims 50, 61, and 65 include limitations similar to those recited in claims 1 and 18 and discussed above, and were rejected for the same reasons as claims 1 and 18. Therefore, the arguments presented above apply with equal force to these claims, as well.

Applicants assert that numerous ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

## CONCLUSION

Applicants submit the application is in condition for allowance, and an early notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-32301/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: September 28, 2009